UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/266,207	03/10/1999	PAUL ENGLAND	777.215US1	5470

22801 7590 08/13/2003

LEE & HAYES PLLC
421 W RIVERSIDE AVENUE SUITE 500
SPOKANE, WA 99201

EXAMINER
KLIMACH, PAULA W

ART UNIT	PAPER NUMBER
2131	12

DATE MAILED: 08/13/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/266,207	Applicant(s) ENGLAND ET AL.
	Examiner Paula W Klimach	Art Unit 2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *29 April 2003* .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-77* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-77* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☒ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) *12* .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

Specification

1. The disclosure is objected to because of the following informalities:

The use of the trademark's AEGIS, IBM's Cryptolop, and A2b has been noted in this application. They should be capitalized wherever it appears and be accompanied by the generic terminology. Capitalize each letter of the word in the bracket or include a proper trademark symbol, such as ™ or © following the word.

Although the use of trademarks is permissible in patent application, the proprietary nature of the marks should be respected and every effort made to prevent their use in any manner, which might adversely affect their validity as trademarks

Appropriate correction is required.

2. **Claim 58** objected to under 37 CFR 1.75(c), as being of improper dependent form for failing to further limit the subject matter of a previous claim. Applicant is required to cancel the claim(s), or amend the claim(s) to place the claim(s) in proper dependent form, or rewrite the claim(s) in independent form. Claim 58 is dependent on claim 62, which is identical to claim 58 and therefore is not limited by claim 58. In addition claim 62 is greater than claim 58 therefore comes after claim 58. All dependent claims must refer to previous claim.

Appropriate correction is required.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. **Claims 1-4, 7, 9-12, 15, 17-19, 22, 25, 32, 30, 35, 40, 41, 43-54, 56-58, 69, 73, and 76** are rejected under 35 U.S.C. 102(e) as being anticipated by Barr et al (6,189,100 B1).

The applied reference has a common assignee with the instant application. Based upon the earlier effective U.S. filing date of the reference, it constitutes prior art under 35 U.S.C. 102(e). This rejection under 35 U.S.C. 102(e) might be overcome either by a showing under 37 CFR 1.132 that any invention disclosed but not claimed in the reference was derived from the inventor of this application and is thus not the invention "by another," or by an appropriate showing under 37 CFR 1.131.

4. *In reference to claim 1*, Barr discloses a computer system having a central processing unit (CPU, Fig. 1 20) and an operating system (OS, Fig. 1 35), the CPU having a software identity register (column 7 lines 59-63), a method for booting the operating system comprising (Fig. 1): computing a cryptographic function of at least a portion of the operating system (column 8 lines 25-35); and setting the software identity register to a result of the computed cryptographic function (column 7 lines 59-63).

5. *In reference to claim 2*, Barr discloses further a method comprising defining a secure storage space, access to which is based in part on the result set in the software identity register (column 7 lines 59-63).

6. *In reference to claim 3*, In a computer system having a central processing unit (CPU) and an operating system (OS), the CPU having a software identity register (column 9 lines 63-67), a method for booting the operating system comprising: executing an atomic operation to set an identity of the operating system into the software identity register of the CPU (column 9 lines 10-18), wherein in an event that the atomic operation completes correctly, the software identity register contains the identity of the operating system and in an event that the atomic operation fails to complete correctly (column 9 lines 24-33), the software identity register contains a value other than the identity of the operating system (column 7 lines 59 to column 8 line 16 in combination with column 8 lines 55-60); and examining a content of the software identity register to verify the identity of the operating system (column 8 lines 25-35).

7. *In reference to claims 4, 9, 10, 12, 17, 18, and 72*, the identity comprises a public key of a correctly signed block of code from the operating system, and examining a content of the software identity register comprises verifying a signature of the signed block of code against the public key (column 9 lines 50-55 in combination with Fig. 7A).

8. *In reference to claim 11*, Barr suggests a computer system having a central processing unit (CPU) and an operating system (OS) (column 4 lines 38-50), the CPU having a software identity register (column 7 lines 59-63), a method comprising: identifying a boot block of code in the OS that uniquely describes the OS (Fig. 7A, step 707 and 717); creating an identity of the OS from the boot block (Fig. 7A step 707); and executing an atomic operation to set the identity of

the operating system into the software identity register of the CPU, wherein in an event that the atomic operation completes correctly, the software identity register contains the identity of the operating system (column 7 lines 59-63 in combination with Fig. 3).

9. *In reference to claims 19, 26, 41, 44,46, 47, and 75*, Barr suggests a computer system having a central processing unit (CPU) and an operating system (OS), the CPU having a pair of private and public keys and a software identity register that holds an identity of the operating system (Fig. 1 in combination with column 7 lines 59-63), a method comprising: creating an identity of the OS containing the identity from the software identity register, information describing the operating system, and the CPU public key (column 9 lines 5-10); and signing the OS certificate using the CPU private key (column 9 lines 50-55).

10. *In reference to claims 7, 15, 22, 25, 30, 31, 32, 34, 35, 38, 40, 43, 45, 48-54, 56-58, 69, 73, and 76,* Barr suggests method for establishing a chain of trust between a subscriber unit and a content provider, the subscriber unit having a central processing unit (CPU) and an operating system (OS), the CPU having a pair of private and public keys (column 9 lines 10-24), a manufacturer certificate supplied by a manufacturer of the CPU (column 9 lines 50-55), and a software identity register that holds an identity of the operating system (column 9 lines 10-23), the method comprising: submitting a request from the subscriber unit to the content provider, the request specifying a particular content (Fig. 7A); generating, at the content provider, a challenge nonce (Fig. 7A); returning the challenge nonce from the content provider to the subscriber unit (Fig. 7A); forming, at the subscriber unit, an OS certificate containing the identity from the software identity register, information describing the operating system, the challenge nonce, and the CPU public key and signing the OS certificate using the CPU private key (column 9 lines 10-

23); passing the OS certificate and the CPU manufacturer certificate from the subscriber unit to the content provider (column 9 lines 50-55); and evaluating, at the content provider, the OS certificate and the CPU manufacturer at the content provider to determine whether to reject or fulfill the request (column 9 lines 50-55 in combination with column 8 lines 17-24).

11. *In reference to claim 36*, the identity comprises a digital signature on a block of code from the operating system (column 6 lines 37-39).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

12. **Claims 5, 13, 33, and 37** are rejected under 35 U.S.C. 103(a) as being unpatentable over Barr in view of Angelo (5,944,821).

Barr does not expressly disclose the operating system's identity comprising a hash digest of a block of code from the operating system, and examining a content of the software identity register comprises hashing the block of code.

Angelo discusses a hash value generated by an integrity assessment code that is specific to a given software application although the disclosed embodiment of the invention utilizes a hash table 206 containing hash values generated by a secure hash algorithm 208, it is

contemplated that many types of modification detection codes could be utilized. Of importance to the invention is that each piece of software to be tracked has a corresponding and fairly unique value that represents the unaltered state of the software, and that this value be stored in a secure memory location (Fig. 3).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to calculate the hash value as an identity and examine the software integrity using the hash value as disclosed by Angelo in the system disclosed by Barr. One of ordinary skill in the art would have been motivated to do this because it is intended to be computationally infeasible to modify data so as to preserve a specific modification detection code value.

13. *In reference to claim 33*, wherein forming a generator key and generating a storage key comprises creating a storage key SK using the formula SK = SHA(CPU-specific secret, OS-specific data, seed). Angelo suggests the calculation of a hash value from a hash algorithm (Fig. 2 in combination with Fig. 3).

14. **Claim 6, 8, 14, 16, 21, 23, 24, 39, 42, 55, and 59-62, and 71** are rejected under 35 U.S.C. 103(a) as being unpatentable over Barr as applied to claims 3, 11, 19, 22, and 35 respectively above, and further in view of Sadowsky et al (6,230,285 B1).

15. *In reference to claims 6, 8, 14, 16, 24, 39, 42, 55, 59-62*, Barr does not expressly disclose maintaining a boot log.

Sadowsky discloses maintaining a boot log (Fig 4). Further Sadowsky suggest the boot file comprising appending at least a portion of the identity to a boot log (column 4 lines 65 and 66).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to append the identity to the boot log of Sadowsky in the system of Barr. One of ordinary skill in the art would have been motivated to do this because it will show the cause of boot failure (column 5 lines 12-15).

16. *In reference to claims 21, 23, and 71*, the method wherein creating an identity of the OS comprises forming the OS certificate with one or more items from a boot log containing identities of software components that are executing on the CPU. The boot log discussed by Sadowsky contains information such as the device driver and executables (column 4 lines 65 and 66). This information is shared with the certificate information suggested by Barr.

17. **Claims 63-68, 74, and 77** are rejected under 35 U.S.C. 103(a) as being unpatentable over Barr as applied to claims 19, 56, 73, and 76 above, and further in view of LeBourgeois (6,026,166).

18. *In reference to claims 63 and 64*, Barr does not expressly disclose the certificate containing the identities of the device drivers.

LeBourgeois discloses the digital certification method where the signature is dependent on the user identity (column 3 lines 54-57). In this case the user would be the device driver of the CPU.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to bind the identification of the device drive to the signature of the certificate as in LeBourgeois in the system of Barr. One of ordinary skill in the art would have been motivated

to do this because it is useful in ensuring that digital products are authorized for use on only one machine (column 3 lines 21-23).

19. *In reference to claim 65 and 66*, LeBourgeois further discloses submitting, by the user computer, a request to the third party (the certificate server) for access to specific content; evaluating, by the third party, whether to permit access based on the level of trust associated with the user computer (Fig. 3B).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to send the request to a certificate server for access to specific content as disclosed by LeBourgeois in the system of Barr. One of ordinary skill in the art would have been motivated to do this because the certificate server will prevent an imposter from creating a message purportedly from the original sender (column 1 lines 22-59)

20. *In reference to claims 67 and 68*, the access comprises transmitting, from the third party (the certificate server), a storage key for the specific content to the user computer through the secure connection (the connection between the merchant and the certificate server), wherein the specific content was previously stored on the user computer (Fig 3A and 3B). The specific content was obtained outside the secure connection (the user system; Fig. 3A).

21. *In reference to claims 20, 70, 74, and 77*, LeBourgeois further suggests submitting the signed software identity register (the identity of the user) over a network to a third party to prove an identity of the operating system to the third party (Fig 3A and Fig. 3B).

22. **Claims 27-29** are rejected under 35 U.S.C. 103(a) as being unpatentable over Barr as applied to claim 22 above, and further in view of Barlow et al (6, 038, 551).

Barr discloses the use of certificates for the operating system, however does not expressly disclose the use of a manufacturing certificate.

Barlow discloses the use of a manufacturing certificate to verify the manufacturer and therefore whether to trust the manufacturer (column 8 line 66 to column 9 line 20).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to compare the manufacturer certificate and the operating system certificate. One of ordinary skill in the art would have been motivated to do this because to prevent possible covert attacks from malicious software applications which attempt to gain unauthorized access to resources on the IC card (column 8 line 66 to column 9 line 3).

Conclusion

23. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Barr et al	6, 189, 100 B1
Angelo	5, 944, 821
Barlow	6, 038, 551
LeBourgeois	6, 026, 166
Sadowsky et al	6, 230, 285

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paula W Klimach whose telephone number is (703) 305-8421. The examiner can normally be reached on Mon to Fri 7:15 a.m to 3:45 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (703) 305-9648. The fax phone numbers for the organization where this application or proceeding is assigned are (703) 305-8421 for regular communications and (703) 305-8421 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-4832.

PWK
August 4, 2003

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100